{REDACTED} Remediation Requirements Outline

Prepared for

by Sean Cooper, on behalf of

Table of Contents

Revision Control Log

Date	Old Version #	New Version #	Revised By:	Description
Sept 30, 2014	0.0	0.1	Sean Cooper	Initial Document Composition
Oct 1, 2014	0.1	0.2	Sean Cooper	Client Discussion WRT Content.
{DATE}	0.1	1.0	Sean Cooper	Final Document Delivery

CONFIDENTIAL

Information Compliance Matrix – Detail Status

TIFIER	STATUS						
'U Line Item #	Compliant	Not Applicable	In-Progress	Planned	Deficient	Information Needed	Dc
1							
2					X		
3							
4					X		
5							
6							
7							
8							
9					X		
10					X		
11							
12					X		
13					X		
14						X	
15	X						
16					X		
17					X		
18						X	
19							
20		X					
21					X		
22	X						
23	X						
24						X	
25						X	
26							
27							
28					X		
29						X	
30							
31					X		
32	X						
33					X		
34					X		
35		X					
36		X					
37		X					
38							
39		X					
40		X					
41		X					
42							

Evaluation Status Criteria

Does Not Exist

Artifact describing policy, procedure, technology or role simply doesn't exist or can't be located.

Information Needed

Attestation has been given that a policy, procedure, technology or role exists, but is awaiting furnishment.

Deficient

Artifact describing policy procedure, technology or role exists, but is rudimentary in nature or missing key features or aspects.

Planned

Artifact describing policy, procedure, technology or role exists and meets all key criteria for industry standards and its implementation has been scheduled but not performed.

In-Progress

Artifact describing policy, procedure, technology or role exists, and its implementation has been scheduled and is currently being performed.

Not Applicable

Requirement is not applicable to this line of business.

Compliant

Artifact describing policy, procedure, technology or role exists and meets all key criteria for industry standards, and the required implementation has been completed and verified.

Remediation Requirements

1. Internal Roles, Policies and Procedures
    a. Formal Risk Assessment Program
    b. Information Security Policies & Procedures
    c. Information Security Oversight Function
2. Asset Management
    a. Asset Management Program
    b. Information Classification Policy
3. Human Resource Security
    a. Background Screening
    b. Confidentiality Agreement / Non-Disclosure Agreement / Information Security Agreement
4. Physical Security
    a. Physical Security Policy
        i. Visitor Log
        ii. Visitor Escorts
        iii. Visitor Identification
    b. Physical Access Protections
        i. Security Guards
        ii. Electronic Access Controls
        iii. Biometric Access Controls
        iv. Periodically Reviewed Access Lists
        v. Closed-Circuit Television Monitoring
        vi. {REDACTED} Data Security Policy Review
5. Infrastructure Management
    a. Two-tiered Firewall Architecture
    b. Restriction of Public Internet Access
    c. Internal DMZs Separating Networks
    d. ICSA-certified Firewalls
    e. Change Control / Change Management Process
    f. Code / Application Reviews
    g. Segregation and Isolation of Roles and Responsibilities
    h. Two-Man Rule
    i. Periodic Review of Access Lists
    j. Antivirus Installation
        i. Updates
        ii. AV Definitions
        iii. Periodic Scans
        iv. User Disablement
    k. Security Event Logging
        i. Log Event Capture
        ii. Protection from Alteration.
    l. Standard Desktop Configuration
    m. Strandard Server Configuration
    n. Patching and Vulnerability Remediation
    o. IPS/IDS Installation and Configuration
        i. IPS/IDS Alert Response Policy
    p. Formal Remote / Wireless Network Policy

i. Encryption
ii. Hidden SSID
iii. Two-factor Authentication

q. Desktop/Server Encryption
r. Physical Media Policy
i. Audited, approved list of those with access to removable devices.
ii. Re-Use Policy
iii. Disposal Policy

6. Access Control
a. Access Control Policy / Process
i. Request and Approval of User Entitlements
ii. Role-Based Access Control
iii. Unique Username / Password combination requirement.
iv. Restriction/Removal of Default Usernames and Shared Usernames
v. Management Approval Requirement for Required Default Usernames
b. United States Jurisdiction
c. Annual System Access Audit and Review
d. Password Policy
i. Prohibition on sharing passwords
ii. Password change policy (60 days or less)
iii. Length, complexity, composition, history requirements.

7. System Development
a. Formal Vulnerability Assessment and Management Program
i. Requires VA and VM on all systems and devices that have access to {REDACTED} data.
ii. Classifies issues according to severity.
iii. Requires timely remediation based on risk scoring and number of systems impacted.
b. Formal Remote Access Policy
i. Requires multi-factor authentication for access.
ii. Restricted to specific IPs, at specific times of day.

8. Information Security Incident Management
a. Incident Response Policy / Procedure
i. Requirement to report all POTENTIAL incidents.
ii. Implementation Testing Procedures
iii. Notification of clients in the event of a confirmed or suspected breach.
iv. Incident Repost Team with clearly defined roles and responsibilities.

9. Compliance
a. Independent Review of Security Policies, Procedures, Guidelines
i. Plan to remediate deficiencies
b. Privacy Policy
i. Confidentiality of Non-Public Personal Information.
ii. Acknowledgement Screen on Login Banner
c. Data Retention Policy
d. Data Storage Policy